REMARKS

This amendment is being filed in response to an Office Action mailed 10/25/2006, in which the Examiner the that claims 37-62 were pending but rejected, and that claims 38-49 and 51-62 were objected to. In this amendment, claims 38, 41, 45-47, 49, 51, 58-60, and 62 are amended to overcome reasons for objections and rejections given by the Examiner, and other objections are traversed below.

A minor correction is applied herein to claim 41, with an extraneous semicolon (;) being eliminated.

In claim 47 and 60, "a the entry" is corrected to read "the entry."

Claims to which Objections were made

In the above-mentioned Office Action, the Examiner said that claims 38-49 and 51-62 were objected to because, in claims 38 and 51, "the protected partition is found match a portion" should be changed to "the protected partition is found to match a portion." This change is made herein to claims 38 and 51.

Claims Rejected under 35 USC §103

In the above-mentioned Office Action, the Examiner also said that claims 37 and 50 were rejected as being unpatentable over U.S. Pat. No. 6,026,016 to Gafken, in view of U.S. Pat. No. 5,128,995 to Arnold et al., and further in view of the "Handbook of Applied Cryptography," by Menezes et al., hereinafter referred to as Menezes.

However, the Applicants reiterate the position that a prima facie case of obviousness cannot be made by combining the teachings of Gafken and Arnold et al. to form certain aspects of the Applicants' invention because Gafken teaches against such a combination. Additional arguments regarding this position

are provided below.

In column 3, lines 56-59, Gafken indicates that the system 100, shown in FIG. 1, may also include a storage device 118 such as a hard disk drive. The hard disk drive is shown as storing an operating system 150, including a BIOS update facility 151, and a user interface 155. As described in column 3, lines 38-43, the system 100 also includes a flash memory 115, also referred to as a flash EEPROM. In column 3, line 66, through column 4, line 10, the flash memory 115 is described as including a memory array 130 that is divided into blocks that are individually erasable. The block structure of the flash memory, having individual registers, is further shown in FIG. 3 and described in column 3, lines 34-45.

Additionally, in FIG. 2 and in column 5, lines 8-15 and 24-28, a system 200 is shown as including a memory 255, other than the nonvolatile memory 215, with the boot code or other start-up routine being stored in either the memory 255 or the nonvolatile memory. The nonvolatile memory 215 is described as including a memory array 230 arranged in blocks, being a flash memory or another type of nonvolatile memory.

The process of Gafken is described in reference to FIGS. 1, 3, and 5 in columns 12-14. Then, in column 14, lines 54-59, Gafken states, "It will be appreciated by those skilled in the art that, although the example above describes a flash memory used to store boot code, a BIOS or other start-up routine, other types of nonvolatile memories storing other types of information may be used for other embodiments in a similar manner."

The Applicants respectfully submit that the other types of nonvolatile memories do not include a hard disk drive, which is conventionally not called a memory at all, but rather a storage device. Gafken shows and describes systems including hard disk drives, but, in each instance, the process of unlocking portions of the

memory and of performing updates to the information therein is described and shown as being applied only to a memory separate from the hard disk drive. All of the descriptions of the memory being updated include descriptions of a memory array including blocks that can be individually erased.

The claims of Gafken each include a reference to a nonvolatile memory array having one or more blocks of memory cells or to a block of nonvolatile memory cells. Such elements are found in flash memories but not in hard disk drives.

Regarding a reference teaching away from an invention, the Applicants cite *In re Gurley,* 31 USPQ2d 1130, 1131 (Fed. Cir. 1994):

> "A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant."

The Applicants respectfully submit that a person of ordinary skill, reading Gafken would be discouraged from trying to apply its methods to a protected partition within a hard disk drive, and therefore, that the teachings of Gafken and Arnold et al. cannot be combined in the manner suggested by the Examiner.

Without the teachings of Arnold et al., Gafken and Menezes fail to teach, describe, or anticipate the requirements of claim 37 for forming a protected partition within a hard drive of each of the computer systems, for the initialization routine to include instructions causing the protected partition to be locked before the operating system is loaded and for instructions causing information to be stored within a predetermined location to be written within the protected partition.

Without the teachings of Gafken, Arnold et al and Menezes fail to, describe, or anticipate the requirements of claim 37 for establishing a network connecting

each computer system in the plurality of computer systems with a server system; generating an update partition file within the server system; transmitting the update partition file over the network to each computer system in the plurality of computer systems; and storing the update partition file within the predetermined location of each computer system in the plurality of computer systems.

Without the teachings of Arnold et al., Gafken and Menezes fail to teach, describe, or anticipate the requirements of claim 50 for data storage including a hard drive having a protected partition, and for the initialization routine to include instructions causing information stored within the predetermined location to be written within the protected partition after predetermined security procedures have occurred but before the protected partition is locked.

Without the teachings of Gafken, Arnold et al and Menezes fail to, describe, or anticipate the requirements of claim 50 for a server system connected to the network and programmed to generate an update partition file and to transmit the update partition file over the network and for the initialization routine to include instructions causing information stored within the predetermined location to be written within the protected partition after predetermined security procedures have occurred but before the protected partition is locked.

For all these reasons, the Applicants respectfully submit that claims 37 and 50 are patentable under 35 USC §103(a).

The Examiner also said that claims 38-43 and 51-56 were rejected under 35 USC §103(a) as being unpatentable over the combination of Gafken, Arnold et al., and Menezes, and further in view of U.S. Pat. No. 6,088,759 to Hasbun et al. It is noted that adding Hasbun et al. to the combination of Gafken, Arnold et al., and Menezes does not overcome the teaching of Gafken against the formation of such a combination, as described above regarding the rejection of claims 37 and

50. Since these dependent claims merely add limitations to claims 37 and 50, it is believed that claims 38-43, 51-56, and additionally claim 62 are patentable over the combination of Gafken, Arnold et al., and Menezes, and further in view of Hasbun et al.

The Examiner further said that claims 44-58 and 57-61 were rejected under 35 USC §103(a) as being unpatentable over the combination of Gafken, Arnold et al., and Menezes and further in view of U.S. Pat. App. Pub. No. 2001/0039651A1 to Hayashi et al. The Examiner also said that Gafken, Arnold et al., and Menezes failed to disclose encrypting portions of the file separately and verifying each portion individually, but that Hayashi et al teaches a method for providing a variety of software safety by breaking the file into pieces and decrypting each piece separately.

The Applicants respectfully submit that, since claims 44-58 and 57-51 merely add limitations to independent claims 37 and 50, respectively, and since adding the teachings of Hayashi et al. does not overcome the deficiencies of the prior art without the combined teachings of Gafken and Arnold et al. in describing the limitations of claims 37 and 50, as explained in detail above regarding the rejection of claims 37 and 50, it is believed that claims 44-58 and 57-61 are patentable under 35 USC §103(a) for the reasons described above regarding the rejection of claims 37 and 50.

Furthermore, the Applicants respectfully submit that Hayashi et al. merely describes a method for decrypting encoded source code in units so that portions of the decrypted data can be erased before the rest of the data is decoded. The chances of decrypted data being stolen are reduced by the fact that the entire decrypted data is never simultaneously available. The Applicants admit that the idea of decrypting code in blocks or units is known to be hundreds of years old. The nature of the technique used for encryption would generally require that

decryption would be done in this way. However, Hayashi et al. does not disclose a process for verifying the identity or origin of the decrypted source code units, and the Applicants respectfully submit that this is the key part of the Applicants' invention as recited in claim 44. Furthermore, in conventional authentication by digital signatures, as described, for example, by Menezes, a single digital signature is used to verify an entire message; individual digital signatures are not used to verify individual blocks of data.

In the computer system of the Applicants' invention, individual entries are received and stored, being individually authenticated before they are stored within the protected partition. These individual entries may be combined before they are transmitted or after they are received. They may include valid entries and invalid entries. With the Applicants' invention, the valid entries are verified and stored within the protected partition; the invalid entries are not. In this way, a significant advantage is gained over prior art systems.

In the above-mentioned Office Action, the Examiner indicated that the Applicants have argued that Hayashi does not teach individual verification of the source of each entry, but that the features upon which the Applicants rely (i.e., individual verification of the source of each entry) are not recited in the rejected claims.

Regarding this statement by the Examiner, the Applicants respectfully submit that claim 44 and 57 each include requirements for verifying the source of each entry, with the requirements being stated as:

> "the method additionally comprises, following determining that the update partition file is stored within the computing system for updating the protected partition, verifying whether each entry in the plurality of entries within the update partition file has been generated by the server system, and
>
> each entry in the plurality of entries within the update partition file is written to the protected partition only following verification that the entry has been

generated by the server system."

In this amendment, claims 45, 46, 58, and 59 have each been amended to change "the entry" to "each entry in the plurality of entries within the update partition file," clarifying that the process of verifying generation of the entry by the server is performed for each of the entries. Support for this change is found in the specification as filed on page 19, lines 6-17, and in FIG. 6A, where it is noted that the AUTHENTICATE subroutine 128 is called whenever it is determined that there is another entry.

Additionally within this amendment, claim 49 has been corrected to indicate dependence upon claim 48 instead of upon claim 38, and claim 62 has been corrected to indicate dependence upon claim 61, instead of upon claim 51.

Therefore, the Applicants respectfully submit that the combination of Gafken, Arnold et al., Menezes, and Hasbun and further in view of Hayashi et al. does not teach, describe, or otherwise anticipate the requirements of claims 44-46 and 57-59 for the method to include verifying whether each entry in the plurality of entries within the update partition file has been generated by the server system. For this reason, the Applicants submit that claims 44-46 and 57-59 are patentable under 35 USC §103(a) over the combination of Gafken, Arnold et al., Menezes, and Hasbun and further in view of Hayashi et al.

Furthermore, because claims 47-49, as amended herein, merely add limitations to claims 44 and 46, and because claims 60-62, as amended herein, merely add limitations to claims 57-59, the Applicants respectfully submit that claims 47-49 and 60-62 are additionally patentable under 35 USC §103(a) over the combination of Gafken, Arnold et al., Menezes, and Hasbun and further in view of Hayashi et al.

Conclusions

For the reasons described in detail above, the Applicants respectfully submit that the Application, including claims 37-62 is now in condition for allowance, and that action is respectfully requested, with reconsideration and withdrawal of all reasons for rejections and objections.

Respectfully submitted,

Ronald V. Davidge
Registration No. 33,863
Telephone No. 954-344-9880
January 2, 2006